Journal of Integer Sequences, Vol. 24 (2021),
Article 21.1.7

Hypothetical Elite Primes for Mersenne Numbers and Repunits

Amin Witno
Department of Basic Sciences
Philadelphia University
19392 Jordan
awitno@gmail.com

Abstract

We study prime numbers p that have the property that the numbers $(b^q-1)/(b-1)$ are quadratic residues modulo p for all sufficiently large primes q. We give a practical criterion for testing for such primes with respect to the base b and, for certain values of b, we find a connection between these primes and anti-elite primes, i.e., where $b^{2^n}+1$ are quadratic residues modulo p for all large n.

1 Introduction

Aigner [1] called a prime number p *elite* if the Fermat numbers $F_n := 2^{2^n}+1$ are quadratic non-residues modulo p for all sufficiently large values of n. Such primes p play a role in Pepin's primality criterion for Fermat numbers, i.e., that F_n is prime if and only if $p^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.

Müller [5] defined a prime p to be *anti-elite* if the numbers F_n are quadratic residues modulo p for all large n. Despite their name, anti-elite primes are still elite in the sense of being rare, as their elite counterparts are, but without the privilege of having a role in primality testing.

Meanwhile, the counterparts to the Fermat numbers are the Mersenne numbers $M_q := 2^q-1$, where q is a prime. Both Fermat and Mersenne numbers belong to the simplest class of the Cunningham numbers $b^N \pm 1$, in this case with $b=2$, which are of great interest as far as primality and factorization are concerned.

We explored the analogous idea of elite primes with respect to Mersenne numbers in place of the Fermat numbers and noted immediately that if a prime $q = (p-1)k+1$ (with infinitely many choices for k, says Dirichlet's theorem), then clearly $M_q \equiv 1 \pmod{p}$ by Fermat's theorem, hence a quadratic residue. Therefore, a prime p cannot be "elite" with respect to Mersenne numbers, but perhaps p can be "anti-elite," i.e., where M_q is a quadratic residue modulo p for all large primes q.

With this definition, and after establishing a practical computational criterion for finding such primes (Theorem 5), we looked through the primes $p < 10^9$ and found no result except $p = 2$ and 3. So we extended the domain of M_q to include a generalization of Mersenne numbers in the form $M_{b,q} := \frac{b^q-1}{b-1}$, where $b \geq 2$ and q is prime. This time the numerical results, collected in Table 1, were encouraging enough for us to continue with the investigation.

Thus, in this article we study the primes p modulo which $M_{b,q}$ are quadratic residues for all large primes q. Some results relate back to Fermat numbers, presumably not surprising, and with respect to certain bases these primes can also be anti-elite with respect to the generalized Fermat numbers $b^{2^n}+1$.

We should mention that the numbers $M_{b,n}$ in general are also known as repunits, since their base-b representations consist of a string of ones.

2 First observations

Definition 1. For all $b \geq 2$ and $m \geq 1$, we fix the notation

$$M_{b,m} = \frac{b^m - 1}{b-1}.$$

We reserve the variables p, q for prime numbers only, and we use the notation $\left(\frac{a}{p}\right)$ for the Legendre/Jacobi symbol. Now let P stand for the set of all prime numbers, and define

$$P_b = \left\{ p \in P : \left(\frac{M_{b,q}}{p}\right) = +1 \text{ for all sufficiently large primes } q \right\}.$$

(Since the property $p \in P_b$ is hypothetical, perhaps we should call such primes *hypo-elite to the base* b.)

Table 1 displays the elements of P_b up to five billion with $b \leq 10$. They can be obtained using an algorithm based on a criterion for $p \in P_b$ explained in Theorem 5 later in this section, after some preliminary observations.

Theorem 2. *If $p \mid b(b+1)$, then $p \in P_b$. If $2 < p \mid (b-1)$, then $p \notin P_b$. In particular, $2 \in P_b$ for all $b \geq 2$, and $3 \in P_b$ if and only if $b \not\equiv 1 \pmod{3}$.*

b	$p \in P_b$
2	2, 3
3	2, 3, 7, 13, 61, 73, 547, 757, 1093, 4561, 6481, 368089, 398581, 530713, 797161, 42521761, 47763361, 2413941289
4	2, 5, 13, 17, 41, 241, 257, 61681, 65537, 15790321, 4278255361, 4562284561
5	2, 3, 5, 7, 521, 601, 5167, 390001, 234750601
6	2, 3, 7, 31, 97, 101
7	2, 7, 43, 1201, 2801, 117307, 6568801
8	2, 3, 19, 73, 87211, 262657, 18837001
9	2, 3, 5, 13, 41, 73, 757, 1093, 1181, 4561, 6481, 368089, 530713, 797161, 21523361, 42521761, 47763361, 2413941289
10	2, 5, 7, 11, 13, 37, 52579, 459691, 2906161

Table 1: The primes $p \in P_b$ up to $p < 5 \cdot 10^9$ and $2 \leq b \leq 10$.

Proof. Since $M_{b,q} = 1 + b + b^2 + \cdots + b^{q-1}$, then $p \mid b(b+1)$ implies that $M_{b,q} \equiv 1 \pmod{p}$ for all primes $q > 2$. In that case $M_{b,q}$ is a quadratic residue modulo p and $p \in P_b$. Now if $p > 2$ and $p \mid (b-1)$, then $M_{b,q} \equiv q \pmod{p}$. By Dirichlet's theorem, we know there are infinitely many primes q in an arbitrary reduced residue class modulo p, in particular the class of a quadratic non-residue; hence $p \notin M_b$ in this case. The second part of the claim follows as $2 \mid b(b+1)$ and that $\{b-1, b, b+1\}$ is a complete residue system modulo 3. □

Remark 3. In particular, P_b contains all the prime factors of b. Hence, given an arbitrarily large number L, we can find a base b such that $|P_b| \geq L$, e.g., by considering b which is the product of L distinct primes.

Remark 4. It is clear from the definition that we have $p \in P_b$ if and only if $p \in P_B$ for all $B \equiv b \pmod{p}$. Hence, for a fixed prime p, we can identify all the bases b for which $p \in P_b$ once they have been determined up to $b < p$, such as what we have in Table 1. For convenience, based on Theorem 2, we may set $P_1 = \{2\}$ and $P_0 = P$. Then, for instance, we observe from Table 1 that $11 \in P_b$ only for $b = 0$ and 10, so we may conclude that $11 \in P_b$ if and only if $b \equiv 0, 10 \pmod{11}$.

In what follows, the notation $|b|_p$ stands for the multiplicative order of b modulo p.

Theorem 5. *Let $p \nmid b(b-1)$, and let $R = R_{b,p}$ be a reduced residue system modulo $|b|_p$. Then the prime $p \in P_b$ if and only if $M_{b,n}$ is a quadratic residue modulo p for every $n \in R$.*

Proof. The condition $p \nmid b(b-1)$ ensures that $k := |b|_p \geq 2$. If q is a large prime, then q belongs to a residue class modulo k represented by one of the elements in R, say n, so that $M_{b,q} \equiv M_{b,n} \pmod{p}$ since $q \equiv n \pmod{k}$. Conversely by Dirichlet's theorem, for every $n \in R$, we have an infinite class of primes congruent to n modulo k. Thus the condition that $M_{b,n}$ be quadratic residue for all $n \in R$ is sufficient as well as necessary for having $p \in P_b$. □

Furthermore, we can reduce computation by observing that only half the elements of R in the preceding theorem need to be tested:

Theorem 6. *Let $k = |b|_p$, where $p \nmid b(b-1)$, and let $H = \{x : 1 < x < \frac{k}{2},\ \gcd(x,k) = 1\}$. Then the prime $p \in P_b$ if and only if $-b$ and $M_{b,n}$ are quadratic residues modulo p for all $n \in H$.*

For example, every Mersenne prime $M_q \notin P_2$, except $M_2 = 3$, because $\left(\frac{-2}{2^q-1}\right) = \left(\frac{-1}{2^q-1}\right)\left(\frac{2}{2^q-1}\right) = (-1)(+1) = -1$. As for primes $M_{b,q}$ in general bases, we do have some positive results stated in the next theorem.

Proof. Let $R = \{x : 1 \leq x \leq k,\ \gcd(x,k) = 1\}$. By Theorem 5, we have $p \in P_b$ if and only if $\left(\frac{M_{b,n}}{p}\right) = +1$ for all $n \in R$. Note that as n ranges through elements of R, so does $k - n$, only in reverse order. Moreover,

$$\frac{b^n - 1}{b - 1}\,(-b^{k-n}) = \frac{-b^k + b^{k-n}}{b-1} \equiv \frac{b^{k-n} - 1}{b - 1} \pmod{p}.$$

Therefore,

$$\left(\frac{M_{b,n}}{p}\right)\left(\frac{M_{b,k-n}}{p}\right) = \left(\frac{-b^{k-n}}{p}\right) = \left(\frac{-b^{k+n}}{p}\right) = \left(\frac{-b^n}{p}\right).$$

Now if n is odd, then $\left(\frac{-b^n}{p}\right) = \left(\frac{-b}{p}\right)$. But if n is even, then k is odd, in which case $k \mid \frac{p-1}{2}$ since $k \mid (p-1)$ by Fermat's theorem. It would follow that $\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \equiv +1 \pmod{p}$, so again $\left(\frac{-b^n}{p}\right) = \left(\frac{-b}{p}\right)$. We have shown that for all $n \in R$,

$$\left(\frac{M_{b,n}}{p}\right)\left(\frac{M_{b,k-n}}{p}\right) = \left(\frac{-b}{p}\right).$$

In particular, if $\left(\frac{-b}{p}\right) = -1$, then $M_{b,k-1}$ is a non-residue modulo p and $p \notin P_b$. But if $\left(\frac{-b}{p}\right) = +1$, then $\left(\frac{M_{b,k-n}}{p}\right) = \left(\frac{M_{b,n}}{p}\right)$, in which case the set R may be replaced by $R \cap \{1, 2, \ldots, \lfloor \frac{k}{2} \rfloor\}$. The case $n = 1$ is trivially redundant, as is the case $\frac{k}{2} \in R$, which can occur only when $k = 2$ and $n = 1$. □

Remark 7. The necessary condition $\left(\frac{-b}{p}\right) = +1$ translates into a congruence class criterion on the prime p which, for small b, is not hard to formulate. For $b \leq 10$, these criteria are displayed in Table 2, with the purpose of checking against the primes we have obtained in the first table.

b	Criteria for p such that $\left(\frac{-b}{p}\right) = +1$
2	$p \equiv 1, 3 \pmod{8}$
3	$p \equiv 1 \pmod{6}$
4	$p \equiv 1 \pmod{4}$
5	$p \equiv 1, 3, 7, 9 \pmod{20}$
6	$p \equiv 1, 5, 7, 11 \pmod{24}$
7	$p \equiv 1, 9, 11 \pmod{14}$
8	$p \equiv 1, 3 \pmod{8}$
9	$p \equiv 1 \pmod{4}$
10	$p \equiv 1, 7, 9, 11, 13, 19, 23, 37 \pmod{40}$

Table 2: Congruence condition necessary for the prime $p \in P_b$.

Theorem 8. *Suppose that $b \bmod 4 \in \{0, 3\}$. If $M_{b,q}$ is a prime number, then $M_{b,q} \in P_{b^k}$ for all $k \geq 1$ such that $q \nmid k$.*

Dubner [2] provides us with a table of primes $M_{b,q}$ up to $b = 99$, e.g., for $b = 3$, we can take $q = 3, 7, 13, 71, 103, 541$. The first three of these, corresponding to $p = 13, 1093, 797161$, appear in our Table 1, belonging to both P_3 and P_9.

Proof. We shall show first that for arbitrary m and n with $\gcd(m, n) = 1$,

$$\left(\frac{M_{b,n}}{M_{b,m}}\right) = +1.$$

Note that $M_{b,m} \equiv 1 \pmod{4}$ when $b \bmod 4 = 0$, as well as when $b \bmod 4 = 3$ provided that m is odd. So let us assume now that m is odd. (For m even, we reverse the roles of m and n.) Moreover, similar to what we have seen in the proof of Theorem 6, we have that

$$\left(\frac{M_{b,n}}{M_{b,m}}\right)\left(\frac{M_{b,m-n}}{M_{b,m}}\right) = \left(\frac{-b^n}{M_{b,m}}\right).$$

And since $M_{b,m} \equiv 1 \pmod{4}$, we have

$$\left(\frac{-b^n}{M_{b,m}}\right) = \left(\frac{b}{M_{b,m}}\right)^n = \left(\frac{1}{b}\right)^n = +1,$$

when b is odd, i.e., when $b \equiv 3 \pmod{4}$, as well as when $b \equiv 0 \pmod{4}$ by involving the Kronecker symbol. (In the case $b \equiv 4 \pmod{8}$, the claim holds without further justification, whereas if $b \equiv 0 \pmod{8}$, the same result holds as $M_{b,m} \equiv 1 \pmod{8}$.) It follows that

$$\left(\frac{M_{b,n}}{M_{b,m}}\right) = \left(\frac{M_{b,m-n}}{M_{b,m}}\right).$$

Using the fact that $M_{b,n} \bmod M_{b,m} = M_{b,n \bmod m}$, we then apply the reciprocity law and remainder mod operations to get

$$\left(\frac{M_{b,n}}{M_{b,m}}\right) = \left(\frac{M_{b,n_1}}{M_{b,m}}\right) = \left(\frac{M_{b,m}}{M_{b,n_1}}\right) = \left(\frac{M_{b,n_2}}{M_{b,n_1}}\right) = \cdots$$

where $n_1 = n \bmod m$ or $m - (n \bmod m)$, whichever is odd, and $n_2 = m \mod n_1$ or $n_1 - (m \bmod n_1)$, whichever is odd, etc., in order to maintain $M_{b,n_j} \equiv 1 \pmod 4$, thereby each reciprocal remains free of minus sign. Hence with $\gcd(m,n) = 1$, this process will terminate with $\left(\frac{M_{b,n}}{M_{b,m}}\right) = \cdots = \left(\frac{M_{b,1}}{M_{b,n_t}}\right) = +1$.

Now letting $m = q$, a fixed odd prime, and n be any larger prime, we have proved that if $M_{b,q}$ is prime, then $M_{b,q} \in P_b$. (The case $q = 2$ deals with the prime $p = b + 1$, to which Theorem 2 applies.) As for the base b^k, note the identity $M_{b,kn} = M_{b^k,n} M_{b,k}$. So if $q \nmid k$, then the same arguments as before yield

$$\left(\frac{M_{b^k,n}}{M_{b,q}}\right) = \left(\frac{M_{b,kn}}{M_{b,q}}\right)\left(\frac{M_{b,k}}{M_{b,q}}\right) = (+1)(+1) = +1,$$

establishing the claim. □

Remark 9. We can also show that $M_{b,q} \notin P_b$ in the case $b \equiv 2 \pmod 4$. Note, for instance, when q and $q' \equiv 2 \pmod q$ are primes,

$$\left(\frac{M_{b,q'}}{M_{b,q}}\right) = \left(\frac{M_{b,2}}{M_{b,q}}\right) = \left(\frac{b+1}{M_{b,q}}\right) = -\left(\frac{M_{b,q}}{b+1}\right) = -\left(\frac{1}{3}\right) = -1.$$

This observation agrees with the known fact that the Mersenne numbers M_q cannot be a perfect square, for otherwise the Jacobi symbol would equal $+1$. (An old result by Lebesgue [4] states that $x^m - 1 = y^2$ is not solvable.)

3 Results involving Fermat numbers

Table 1 shows that the Fermat primes $F_m \in P_4$ for $m = 1, 2, 3, 4$. Although it is unknown if there exists another Fermat prime after F_4, we will prove in Corollary 14 that all Fermat primes belong in P_4. Other results in this section concern the idea of a prime being anti-elite with respect to Fermat numbers in general bases:

Definition 10. Recall the generalized Fermat numbers $F_{b,n} = b^{2^n} + 1$. Let a prime p be considered *anti-elite to the base* b if $F_{b,n}$, when sufficiently large, are all quadratic residues modulo p.

Theorem 11. *Fix an even base b, and let $m = 2^s r$, with $0 \le s \le n$ and $2 \nmid r$. The following results apply to the Jacobi symbol $\left(\frac{M_{b,m}}{F_{b,n}}\right)$ with $n \ge 1$.*

1. *For* $s = 0$, *we have* $\left(\frac{M_{b,m}}{F_{b,n}}\right) = +1$ *if* $b \equiv 0 \pmod 4$, *and indeterminate if* $b \equiv 2 \pmod 4$.

2. *For* $s = 1$, *we have* $\left(\frac{M_{b,m}}{F_{b,n}}\right) = +1$ *if* $b \equiv 0, 6 \pmod 8$, *and* $\left(\frac{M_{b,m}}{F_{b,n}}\right) = -1$ *if* $b \equiv 2, 4 \pmod 8$.

3. *For* $s \geq 2$, *we have* $\left(\frac{M_{b,m}}{F_{b,n}}\right) = +1$ *if* $b \equiv 0, 2 \pmod 8$, *and* $\left(\frac{M_{b,m}}{F_{b,n}}\right) = -1$ *if* $b \equiv 4, 6 \pmod 8$.

Proof. The condition $s \leq n$ implies that $\gcd(b^m - 1, b^{2^n} + 1) = 1$. Let us perform Bezout's algorithm for evaluating $\gcd(2^{n-s}, r) = 1$, and where in each iteration we multiply the equation by 2^s:

$$\begin{aligned} 2^n &= (2^s r)u + 2^s r_1 \\ 2^s r &= (2^s r_1)u_1 + 2^s r_2 \\ 2^s r_1 &= (2^s r_2)u_2 + 2^s r_3 \\ &\vdots \\ 2^s r_{t-1} &= (2^s r_t)u_t + 2^s. \end{aligned}$$

Note that $r > r_1 > r_2 > \cdots > r_t > 1$. With these, we apply the reciprocal law to the Jacobi symbol $\left(\frac{b^m-1}{b^{2^n}+1}\right)$ repeatedly,

$$\left(\frac{b^{2^s r} - 1}{b^{2^n} + 1}\right) = \left(\frac{b^{2^n} + 1}{b^{2^s r} - 1}\right) = \left(\frac{b^{2^s r_1} + 1}{b^{2^s r} - 1}\right) = \left(\frac{b^{2^s r} - 1}{b^{2^s r_1} + 1}\right) = \left(\frac{(-1)^{u_1} b^{2^s r_2} - 1}{b^{2^s r_1} + 1}\right)$$

Note that $\left(\frac{-1}{b^{2^s r_1}+1}\right) = +1$. Depending on the parity of u_1, we continue,

$$\left(\frac{(-1)^{u_1} b^{2^s r_2} - 1}{b^{2^s r_1} + 1}\right) = \left(\frac{\pm b^{2^s r_2} - 1}{b^{2^s r_1} + 1}\right) = \left(\frac{b^{2^s r_2} \mp 1}{b^{2^s r_1} + 1}\right) = \left(\frac{b^{2^s r_1} + 1}{b^{2^s r_2} \mp 1}\right).$$

At this point, there are three ways to go with the $+/-$ sign:

$$\left(\frac{b^{2^s r_1} + 1}{b^{2^s r_2} \mp 1}\right) = \left(\frac{b^{2^s r_3} + 1}{b^{2^s r_2} - 1}\right) \quad \text{or} \quad \left(\frac{b^{2^s r_3} + 1}{b^{2^s r_2} + 1}\right) \quad \text{or} \quad \left(\frac{b^{2^s r_3} - 1}{b^{2^s r_2} + 1}\right).$$

In fact, these three are the only possible forms until we reach the t-th iteration, i.e.,

$$\left(\frac{b^{2^s r} - 1}{b^{2^n} + 1}\right) = \left(\frac{b^{2^s} + 1}{b^{2^s r_t} - 1}\right) \quad \text{or} \quad \left(\frac{b^{2^s} + 1}{b^{2^s r_t} + 1}\right) \quad \text{or} \quad \left(\frac{b^{2^s} - 1}{b^{2^s r_t} + 1}\right).$$

We proceed case by case, respectively:

Case 1. Note that here r_t must be odd since we start off with the Jacobi symbol $\left(\frac{b^m-1}{b^{2^n}+1}\right)$ having $\gcd(b^m - 1, b^{2^n} + 1) = 1$. Hence,

$$\left(\frac{b^{2^s} + 1}{b^{2^s r_t} - 1}\right) = \left(\frac{b^{2^s r_t} - 1}{b^{2^s} + 1}\right) = \left(\frac{(-1)^{r_t} - 1}{b^{2^s} + 1}\right) = \left(\frac{-2}{b^{2^s} + 1}\right).$$

Case 2. This time, r_t is even:

$$\left(\frac{b^{2^s}+1}{b^{2^s r_t}+1}\right) = \left(\frac{b^{2^s r_t}+1}{b^{2^s}+1}\right) = \left(\frac{(-1)^{r_t}+1}{b^{2^s}+1}\right) = \left(\frac{2}{b^{2^s}+1}\right).$$

Case 3. Similarly,

$$\left(\frac{b^{2^s}-1}{b^{2^s r_t}+1}\right) = \left(\frac{b^{2^s r_t}+1}{b^{2^s}-1}\right) = \left(\frac{2}{b^{2^s}-1}\right).$$

From all these we collect the following results.

1. For $s = 0$, we have $\left(\frac{b^m-1}{b^{2^n}+1}\right) = +1$ if $b \equiv 0 \pmod 8$, and $\left(\frac{b^m-1}{b^{2^n}+1}\right) = -1$ if $b \equiv 4 \pmod 8$, and indeterminate if $b \equiv 2 \pmod 4$.

2. For $s = 1$, we have $\left(\frac{b^m-1}{b^{2^n}+1}\right) = +1$ if $b \equiv 0 \pmod 4$, and $\left(\frac{b^m-1}{b^{2^n}+1}\right) = -1$ if $b \equiv 2 \pmod 4$.

3. For $s \geq 2$, we have $\left(\frac{b^m-1}{b^{2^n}+1}\right) = +1$ in all cases.

We also verify easily that $\left(\frac{b-1}{b^{2^n}+1}\right) = +1$ if $b \equiv 0, 2 \pmod 8$, and $\left(\frac{b-1}{b^{2^n}+1}\right) = -1$ if $b \equiv 2, 4 \pmod 8$. Lastly, we use the relation $\left(\frac{M_{b,m}}{F_{b,n}}\right) = \left(\frac{b^m-1}{b^{2^n}+1}\right)\left(\frac{b-1}{b^{2^n}+1}\right)$ to put together the desired claim. □

Corollary 12. *Suppose that $b \equiv 0 \pmod 4$. Then $\left(\frac{M_{b,q}}{F_{b,n}}\right) = +1$ for any odd number q. Hence, if $F_{b,n}$ is prime, then $F_{b,n} \in P_b$. In reciprocal, if $M_{b,q}$ is prime, then $M_{b,q}$ is anti-elite to the base b.*

Remark 13. This corollary is the case $s = 0$ in Theorem 11. Primes $M_{b,q}$, being scarce, are typically discovered having large values of q. Now, since Fermat numbers are recursive, they are periodic modulo p. In the case of $p = M_{b,q}$, the period length is given by $|2|_q$, hence expectedly large too. For instance, the fourteenth repunit prime base 12, according to A004064 in OEIS [6], is $M_{12,769543}$. Since 12 is a multiple of 4, this prime is anti-elite to this base with period $|2|_{769543} = 384771$.

Corollary 14. *Suppose that $F_{b,n}$ is a prime number for some $n \geq 1$. If $b \equiv 0 \pmod 4$, then $F_{b,n} \in P_{b^k}$ for all $k \geq 1$ such that $2^{n+1} \nmid k$. If $b \equiv 2 \pmod 4$, then $F_{b,n} \in P_{b^{2k}}$ for all $k \geq 1$ such that $2^n \nmid k$. In particular, all Fermat primes $F_n \in P_{4^k}$ for all such k.*

Proof. The identity $M_{b,km} = M_{b^k,m} M_{b,k}$ gives $\left(\frac{M_{b^k,m}}{F_{b,n}}\right) = \left(\frac{M_{b,km}}{F_{b,n}}\right)\left(\frac{M_{b,k}}{F_{b,n}}\right)$. Note that if m is odd, the factor of 2 dividing k and km are of the same multiplicity. In that case $\left(\frac{M_{b,km}}{F_{b,n}}\right) = \left(\frac{M_{b,k}}{F_{b,n}}\right)$ by Theorem 11, provided that we require k to be even when $b \equiv 2 \pmod 4$ in order to avoid the indeterminate case. Hence, $\left(\frac{M_{b^k,q}}{F_{b,n}}\right) = +1$ for all odd prime q. □

Remark 15. We can extend the proof of Theorem 11 to include $\left(\frac{M_{b^k,m}}{F_{b,n}}\right) = +1$ if m is even, provided that k is also even, or a multiple of 4 when $b \equiv 2 \pmod 4$. In particular, with

$m = 2$ and $k = 2^r$, we have $M_{b^{2^r},2} = F_{b,r}$. Then $\left(\frac{F_{b,n}}{F_{b,r}}\right) = \left(\frac{F_{b,r}}{F_{b,n}}\right) = +1$ for all $n > r$. Hence, we can show that generalized Fermat primes $F_{b,r}$, for $r \geq 2$, are anti-elite to their own base. However, this is a fact already known [5] and easy to obtain due to the relation $F_{b,n} \equiv 2 \pmod{F_{b,r}}$ for all $n > r$. And unfortunately, no other anti-elite primes can be identified in this manner as it has been observed that $M_{b,q}$ is always composite when b is a perfect power, except possibly for $q = 2$, i.e., the Fermat primes already considered.

We do not observe a general pattern for odd bases b. The following theorem deals with an isolated result for $b = 3$.

Theorem 16. *If the number $\frac{F_{3,n}}{2}$ is prime, then $\frac{F_{3,n}}{2} \in P_{9^k}$ for all k odd.*

Primes of the form $\frac{F_{3,n}}{2}$ are currently known with $n = 0, 1, 2, 4, 5, 6$ [A275377]. Four of these are included in Table 1, belonging in P_9.

Proof. We exclude $n = 0$, although it is valid, and introduce the notation $E_r = \frac{9^r+1}{2}$. Hence $\frac{F_{3,n}}{2} = E_{2^{n-1}}$. Note the following facts.

1. We have $E_r \equiv 1 \pmod 4$ for all $r \geq 0$.
2. The number $M_{9,m}$ is odd only when m is odd.
3. We have $\gcd(E_{2^{n-1}}, M_{9,m}) = 1$ for all $n \geq 1$ when m is odd.

We first show that $\left(\frac{M_{9,m}}{E_{2^{n-1}}}\right) = +1$ for all odd m, then it would follow that $\left(\frac{M_{9^k,m}}{E_{2^{n-1}}}\right) = \left(\frac{M_{9,km}}{E_{2^{n-1}}}\right)\left(\frac{M_{9,k}}{E_{2^{n-1}}}\right) = (+1)(+1) = +1$ for all odd k.

Let us fix an odd m, and let $r_1 = 2^{n-1} \bmod m$. By the congruence $9^m \equiv 1 \pmod{M_{9,m}}$, we get

$$\left(\frac{E_{2^{n-1}}}{M_{9,m}}\right) = \left(\frac{2}{M_{9,m}}\right)\left(\frac{9^{2^{n-1}}+1}{M_{9,m}}\right) = \left(\frac{2}{M_{9,m}}\right)\left(\frac{9^{r_1}+1}{M_{9,m}}\right) = \left(\frac{E_{r_1}}{M_{9,m}}\right).$$

Now by the congruence $9^{r_1} \equiv -1 \pmod{E_{r_1}}$, this Jacobi symbol equals to

$$\left(\frac{M_{9,m}}{E_{r_1}}\right) = \left(\frac{8}{E_{r_1}}\right)\left(\frac{9^m-1}{E_{r_1}}\right) = \left(\frac{8}{E_{r_1}}\right)\left(\frac{\pm 9^{r_2}-1}{E_{r_1}}\right),$$

where $r_2 = m \bmod r_1$. In the plus case, we have

$$\left(\frac{E_{2^{n-1}}}{M_{9,m}}\right) = \left(\frac{8}{E_{r_1}}\right)\left(\frac{9^{r_2}-1}{E_{r_1}}\right) = \left(\frac{M_{9,r_2}}{E_{r_1}}\right) = \left(\frac{E_{r_1}}{M_{9,r_2}}\right),$$

noting that if r_2 is even, then the Jacobi symbol is temporarily replaced by Kronecker symbol. Similarly, in the minus case,

$$\left(\frac{E_{2^{n-1}}}{M_{9,m}}\right) = \left(\frac{8}{E_{r_1}}\right)\left(\frac{-9^{r_2}-1}{E_{r_1}}\right) = \left(\frac{2}{E_{r_1}}\right)\left(\frac{9^{r_2}+1}{E_{r_1}}\right) = \left(\frac{E_{r_2}}{E_{r_1}}\right) = \left(\frac{E_{r_1}}{E_{r_2}}\right).$$

This process terminates, say at the t-th iteration, having produced the remainders $r_1 > r_2 > \cdots > r_t > 1$. Observe that there are only three possible final forms.
Case 1. We have $\left(\frac{E_{2^n-1}}{M_{9,m}}\right) = \cdots = \left(\frac{M_{9,1}}{E_{r_t}}\right) = +1$.
Case 2. The case where we must have r_t odd, since $\gcd(E_{2^{n-1}}, M_{9,m}) = 1$:

$$\left(\frac{E_{2^{n-1}}}{M_{9,m}}\right) = \cdots = \left(\frac{E_1}{M_{9,r_t}}\right) = \left(\frac{M_{9,r_t}}{5}\right) = \left(\frac{8}{5}\right)\left(\frac{9^{r_t}-1}{5}\right) = -\left(\frac{-2}{5}\right) = +1.$$

Case 3. The last case, where we would have r_t even:

$$\left(\frac{E_{2^{n-1}}}{M_{9,m}}\right) = \cdots = \left(\frac{E_1}{E_{r_t}}\right) = \left(\frac{5}{E_{r_t}}\right) = \left(\frac{2}{5}\right)\left(\frac{9^{r_t}+1}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = +1.$$

And the proof is complete. □

Our last observation in connection with anti-elite primes is irrespective of the family to which the prime p belongs, but is given by the multiplicative order of the base b.

Theorem 17. *Suppose that $|b|_p$ is an odd number. If $p \in P_b$, then p is anti-elite to the base b.*

Table 1 contains quite a number of occurrences with odd $|b|_p$, thus anti-elite primes, e.g., 2906161 in base 10 and 2413941289 in base 3, as well as the repunit $M_{3,13} = 797161 \in P_3$.

Proof. Note that $F_{b,n}\, M_{b,2^n} = M_{b,2^{n+1}}$ and that $\gcd(2^n, |b|_p) = 1$ for all n. Hence, if $p \in P_b$, then by Theorem 5, both $M_{b,2^n}$ and $M_{b,2^{n+1}}$ are quadratic residues modulo p, and so is $F_{b,n}$. □

Corollary 18. *Every repunit prime $M_{b,q}$ is anti-elite to its base, if $b \equiv 0, 3 \pmod 4$.*

Proof. The case $b \bmod 4 = 0$ overlaps with Corollary 12. Regardless, for these two classes of b, we have $M_{b,q} \in P_b$ if prime, by Theorem 8. Such an event comes with $|b|_{M_{b,q}} = q$, which is necessarily an odd prime. □

4 For further research

This has been an initial investigation on primes p elements of P_b, i.e., such that $\left(\frac{M_{b,q}}{p}\right) = +1$ for all large primes q, and motivated by the search for new insight into elite/anti-elite primes. If the subject is proven worthwhile, we would invite the readers to look into the infinitude of P_b, for all or specific values of b. The facts that some P_b can be large (Remark 3) and that some contain repunit primes naturally suggest that there may indeed be infinitely many such primes for a fixed base. However, our numerical data also suggest that we may have a convergent reciprocal sum $\sum_{p \in P_b} 1/p$, in line with the reciprocal sum of elite primes, which has been proved convergent by Křížek et al. [3].

References

[1] A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatschen Zahlen quadratische Nichtreste sind, *Monatsh. Math.* **101** (1986), 85–93.

[2] H. Dubner, Generalized repunit primes, *Math. Comp.* **61** (1993), 927–930.

[3] M. Křížek, F. Luca, and L. Somer, On the convergence of series of reciprocals of primes related to the Fermat numbers, *J. Number Theory* **97** (2002), 95–112.

[4] M. Lebesgue, Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2+1$, *Nouvelles Annales de Mathématiques 1re série* **9** (1850), 178–181.

[5] T. Müller, On anti-elite prime numbers, *J. Integer Sequences* **10** (2007), Article 07.9.4.

[6] N. J. A. Sloane et al., The On-Line Encyclopedia of Integer Sequences, `https://oeis.org`, last accessed January 2021.

2020 *Mathematics Subject Classification*: Primary 11A15; Secondary 11A41.
Keywords: Fermat number, Mersenne number, generalized repunit, elite prime.

(Concerned with sequences A004064, A102742, A128852, and A275377.)

Received August 4 2020; revised version received January 2 2021. Published in *Journal of Integer Sequences*, January 3 2021.

Return to Journal of Integer Sequences home page.